IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:	Myles Jordan
Serial No.:	09/905,533
Filing Date:	July 14, 2001
Group Art Unit:	2137
Confirmation No.:	3486
Examiner:	Kevin R. Schubert
Title:	DETECTION OF DECRYPTION TO IDENTIFY ENCRYPTED VIRUS

Mail Stop AF
Commissioner For Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

Dear Sir:

PRE-APPEAL BRIEF REQUEST FOR REVIEW

The following Pre-Appeal Brief Request for Review ("Request") is being filed in accordance with the provisions set forth in the Official Gazette Notice of July 12, 2005 ("OG Notice"). Pursuant to the OG Notice, this Request is being filed concurrently with a Notice of Appeal. Applicant respectfully requests reconsideration of the rejection of all claims in the Application.

REMARKS

In the prosecution of the present Application, the Examiner's rejections and assertions contain clear errors of law. Most notable of the legal errors present in the examination of the Application is a failure of the Final Office Action to establish a *prima facie* rejection of the claims in the Application under 35 U.S.C. § 103. The Final Office Action rejected Claims 1, 2, 7-12, and 17-18 under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,357,008 to Nachenberg ("*Nachenberg I*") in view of U.S. Patent No. 6,453,345 to Trcka ("*Trcka*"). These rejections, however, fail to meet the required *prima facie* standard for rejections for the reasons set forth below.

Independent Claim 2 is allowable because the *Nachenberg I-Trcka* proposed by the Examiner fails to disclose, teach, or suggest "triggering a viral detection alarm ***in response to*** determining that one of the listed memory regions is larger than the predetermined size" (emphasis added), recited Claim 2.

Independent Claim 2 is allowable over the *Nachenberg I-Trcka* combination proposed by the Examiner because the Examiner has improperly picked features from the references to the exclusion of the teachings of the remainder of such references. To this end, Applicant respectfully provides the reminder that in making a determination of obviousness, "the prior art ***as a whole*** must be considered. The teachings are to be viewed as they would have been viewed by one of ordinary skill." *In re Hedges,* 783 F.2d 1038, 1041, 228 USPQ 685, 687 (Fed. Cir. 1986) (emphasis added). "It is impermissible within the framework of section 103 to ***pick and choose*** from any one reference only so much of it as will support a given position, to the exclusion of other parts necessary to the full appreciation of what such reference fairly suggests to one of ordinary skill in the art" (emphasis added). *Id.*

The Examiner claims that *Trcka* teaches "triggering a viral detection alarm" and *Nachenberg I* teaches "determining that one of the listed memory regions is larger than the predetermined size." (Final Office Action, page 3.) Applicant respectfully argues that even if this were the case, the references still fail to disclose, teach, or suggest "triggering a viral detection alarm ***in response to*** determining that one of the listed memory regions is larger than the predetermined size" (emphasis added), as recited in Claim 2.

Nachenberg I discloses establishing whether a region of a certain size has been decrypted in order to determine when to move from a decryption phase to an exploration phase. According to *Nachenberg I*:

> On the other hand, if the first threshold number has been reached, then the decryption module 152 determines in a fourth procedure 308 whether a region of a certain minimum size or larger appears to have been decrypted. ... ***If no such region appears to have been decrypted***, then under the assumption that any virus present is unlikely to be an encrypted virus, ***the decryption phase 252 ends*** and the exploration phase 254 begins.
>
> On the other hand, ***if such a region appears to have been decrypted***, then emulation in ***the decryption phase 252 continues*** to allow further decryption by fetching the instruction at the virtual CS:IP in the sixth procedure 312 unless a second threshold number of emulated instructions has been reached.

(*Nachenberg I*, column 8, lines 1-19, emphasis added.) That is, *Nachenberg I* establishes whether a region of a certain size has been decrypted ***merely to determine when to move from the decryption phase, but not to detect computer viruses***.

Trcka discloses triggering an alarm in response to detecting a known virus. According to *Trcka*:

> In one configuration option, the Automated Monitor 140 checks all inbound transfers of executable files for known viruses. By selecting an ALERT MONITOR menu option on the graphical user interface 104, the user can enable and disable various visual and audible event alarms. For example, the user can configure the Automated Monitor 140 to trigger an audible or visual alarm upon detecting a virus in an inbound file transfer.

(*Trcka*, column 17, lines 27-34.) That is, *Trcka* merely discloses triggering an alarm ***in response to detecting a known virus, but not in response to a determination about the size of a memory region***.

Applicant respectfully submits that ***establishing whether a region of a certain size has been decrypted to determine when to move from a decryption phase*** and ***triggering an alarm in response to detecting a known virus*** fail to disclose, teach, or suggest "triggering a viral detection alarm ***in response to*** determining that one of the listed memory regions is larger than the predetermined size" (emphasis added) as recited Claim 2.

Furthermore, *Nachenberg I* teaches away from the *Nachenberg I-Trcka* combination proposed by the Examiner. *Nachenberg I* discloses detecting computer viruses ***based on suspicious behavior***. According to *Nachenberg I*:

> A purpose of the evaluation phase is ***to analyze any suspicious behavior observed during the decryption and exploration phases to determine whether the target appears to be infected***.

(*Nachenberg I*, Abstract, emphasis added.) That is, the *Nachenberg I* method analyzes suspicious behavior to detect computer viruses. Presumably, if the *Nachenberg I* method triggered an alarm, the alarm would be triggered ***in response to detecting suspicious behavior***, but not in response to establishing whether a region of a certain size has been decrypted. Accordingly, *Nachenberg I* teaches away from the *Nachenberg I-Trcka* combination proposed by the Examiner.

Consequently, *Nachenberg I-Trcka* combination fails to disclose, teach, or suggest "triggering a viral detection alarm in response to determining that one of the listed memory regions is larger than the predetermined size," recited Claim 2. Accordingly, independent Claim 2 is allowable over the *Nachenberg I-Trcka* combination.

For at least analogous reasons, independent Claims 1, 7-12, and 17-18 are allowable over the *Nachenberg I-Trcka* combination. Accordingly, Applicant respectfully requests reconsideration and allowance of independent Claims 1, 2, 7-12, and 17-18, and their dependent claims.

CONCLUSION

As a *prima facie* rejection has not been established against Applicants' claims, Applicants respectfully request a finding of allowance of all claims in the Application.

To the extent necessary, the Commissioner is hereby authorized to charge any fees or credit any overpayments to Deposit Account No. 02-0384 of BAKER BOTTS L.L.P.

Respectfully submitted,

BAKER BOTTS L.L.P.
Attorneys for Applicant

Keiko Ichiye
Reg. No. 45,460

KI/ls

Correspondence Address:
Baker Botts L.L.P.
2001 Ross Avenue, Suite 600
Dallas, Texas 75201-2980
(214) 953-6494
Date: June 30, 2006

Customer Number: 05073